Ordine degli Avvocati di Ivrea

Camera Penale "Vittorio Chiusano"
del Piemonte Occidentale e della Valle d'Aosta
Sezione di Ivrea

Aderente all'Unione delle Camere Penali Italiane

Il Consiglio dell' Ordine degli Avvocati di Ivrea
in collaborazione con la Camera Penale "Vittorio Chiusano" Sezione di Ivrea
Organizzano

Incontro di Studio

10 GENNAIO 2020

dalle ore 15:00 alle 18:00 presso la sede in Ivrea, Via Monte Navale, nei locali dell'Officina H, Facoltà di Scienze Infermieristiche

GDPR: nuovi oneri e nuove opportunità per Avvocati e Imprese

Obblighi dell'Avvocato (adeguamento al GDPR)

e

Opportunità per l'Avvocato (servizi resi all'imprese o PA)

Obblighi dell'Avvocato

Ogni Avvocato svolgendo la propria attività professionale quotidiana tratta dati personali (comuni e particolari), dal primo incontro con il cliente fino alla richiesta del pagamento dei propri onorari, diventando così titolare del trattamento dei dati personali che processa

In pratica è colui che decide le **finalità, le modalità ed i mezzi del trattamento** (art. 4 del GDPR)

Sulla base della normativa comunitaria (Regolamento UE 2016/679 e nazionale (Codice privacy «adeguato») l'Avvocato dovrà procedere:

- **Alla nomina del DPO qualora prevista per legge;**
- **istituire il registro delle attività di trattamento, ai sensi dell'art. 30 GDPR;**
- **notificare eventuali *data breach,* con specifiche procedure da attivare in caso di eventuali violazioni;**
- **Rilasciare l'informativa sulla base degli artt. 13 e seguenti GDPR;**
- **Verificare i processi interni allo Studio in tema di trattamento dati, ai sensi dell'art. 24 GDPR, provvedendo a definire in maniera adeguata i ruoli e assicurandosi che tutto il personale riceva adeguata formazione**

- **Verificare i sistemi informatici per assicurare il rispetto dei principi di protezione dei dati;**
- **formalizzare o rinnovare rapporti contrattuali con eventuali responsabili esterni del trattamento dei dati. Si pensi per esempio al commercialista o con la software house;**
- **prevedere nuove specifiche autorizzazioni per i soggetti che trattano i dati, per esempio con l'adozione di livelli di sicurezza distinti in funzione dell'incarico ricoperto;**
- **Verificare l'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio;**
- **Effettuare una valutazione di impatto privacy (DPIA), così come richiesto dalle regole di condotta emanate dal Garante (D.M. 16 marzo 219)**.

In particolare l'Avvocato nel corso del trattamento dovrà verificare che i dati personali siano:

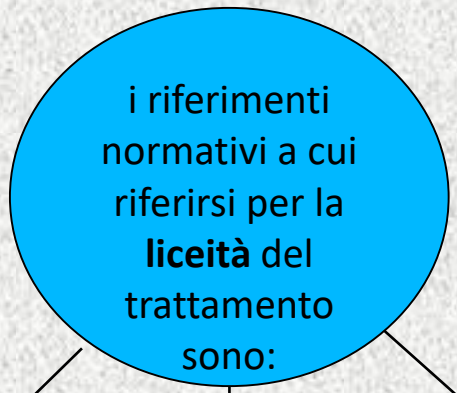
FINALIZZATI	**I dati devono essere pertinenti a quanto necessario per lo scopo del trattamento dichiarato. L'informazione espressa da parte dell'avvocato delle finalità deve precedere l'acquisizione del consenso affinché quest'ultimo sia effettivamente consapevole.**
ACCURATI	**Deve esserci una verifica della correttezza, veridicità e completezza dei dati. L'avvocato è tenuto non solo a trattare dati esatti garantendo quindi la loro qualità, ma deve anche approntare una organizzazione che garantisca il relativo controllo con adozione di tutte le misure necessarie alla rettificazione o cancellazione di dati inesatti**
LIMITATI	**Si devono trattare solo i dati strettamente necessari alle finalità dichiarate nell'informativa.**
UTILIZZATI IN MODO CONFIDENZIALE E RISERVATO	**Anche attraverso l'utilizzo di sistemi di sicurezza (cifratura e anonimizzazione attraverso attribuzione di numero riferimento).**
CONSERVATI (archiviati) non oltre il tempo strettamente necessario	**Si devono trattenere i dati solo per il tempo necessario al conseguimento delle finalità del trattamento e per gli obblighi di legge.**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069653]

Ai sensi dell'art. 20 del D. Lgs. 101/18 il Garante ha verificato la conformità dei Codici di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, statistici, scientifici e **investigazioni difensive** al Regolamento Ue 2016/679 sulla protezione dei dati personali.

Ai sensi dell'art. 2 quater comma 4 del D.Lgs. 196/03
Il rispetto delle Regole Deontologiche costituisce una vera e propria condizione di liceità e correttezza del trattamento



art 6 lett.A-B) → Dati comuni

art. 9 lett.F) → Dati particolari

art. 10 e 2 octies co.3 lett. E) → Dati giudiziari

Il CONSENSO COME CONDIZIONE DI LICEITA'

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli che erano già previsti nel vecchio Codice privacy - d.lgs. 196/2003**

- consenso
- adempimento obblighi contrattuali
- interessi vitali della persona interessata o di terzi
- obblighi di legge cui è soggetto il titolare
- interesse pubblico o esercizio di pubblici poteri
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati

Ambito di applicazione

Le presenti regole deontologiche devono essere rispettate nel trattamento di dati personali per svolgere **investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione**,

da parte di:

a) **avvocati o praticanti avvocati** iscritti ad albi territoriali o ai relativi registri, sezioni ed elenchi, **i quali esercitino l'attività in forma individuale, associata o societaria** svolgendo, anche su mandato, un'attività in sede giurisdizionale o di consulenza o di assistenza stragiudiziale, anche avvalendosi di collaboratori, dipendenti o ausiliari, **nonché da avvocati stranieri esercenti legalmente la professione sul territorio dello Stato**;

b) **soggetti che, sulla base di uno specifico incarico anche da parte di un difensore, svolgano in conformità alla legge attività di investigazione privata** (art. 134 r.d. 18 giugno 1931, n. 773; art. 222 norme di coordinamento del c.p.p.). 2. Le presenti regole deontologiche si applicano, altresì, a chiunque tratti dati personali per le finalità di cui al comma 1, in particolare a altri liberi professionisti o soggetti che in conformità alla legge prestino, su mandato, attività di assistenza o consulenza per le medesime finalità.

Modalità di trattamento

L'avvocato organizza il trattamento **secondo le modalità che risultino più adeguate**, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i princìpi di **finalità, proporzionalità e minimizzazione dei dati**

↓

Attraverso un'attenta **valutazione** sostanziale e non formalistica delle garanzie previste, **nonché di un'analisi** della quantità e qualità delle informazioni che utilizza e **dei possibili rischi (art. 35 GDPR)**

Tali decisioni sono adottate dal titolare del trattamento il quale resta individuato, a seconda dei casi, in:

a) **un singolo professionista**;

b) **una pluralità di professionisti, codifensori della medesima parte assistita** o che, anche al di fuori del mandato di difesa, siano stati comunque interessati a concorrere all'opera professionale quali **consulenti o domiciliatari**;

c) **un'associazione tra professionisti** o una società di professionisti.

Nomina dei Soggetti AUTORIZZATI (ex incaricati)

Il Titolare/Avvocato dovrà impartire per iscritto alle persone **AUTORIZZATE** al trattamento dei dati, concrete indicazioni in ordine alle modalità che tali soggetti dovranno osservare

- **Personale di segreteria;**
- **Collaboratori/tirocinanti;**
- **Sostituti processuali**

Nomina dei Responsabili esterni del Trattamento ex art. 28 GDPR

Ai sensi dell'art. 4, par. 8 il **Responsabile del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che "tratta dati personali **per conto** del titolare del trattamento".

È importante sottolineare il concetto del trattamento dei dati personali "per conto" del titolare del trattamento. Il responsabile, in sostanza, effettua il trattamento in quanto i dati personali gli sono comunicati dal titolare del trattamento.

In pratica, è la persona che tratta dati personali per conto dello studio legale come un contabile, un editore di software, un host web, ecc.

Il responsabile è da considerarsi solo **"esterno"** allo studio legale; pertanto non è possibile nominare un Collega, un dipendente o un collaboratore come responsabile della protezione dei dati.

I soggetti a cui lo studio comunica i dati personali trattati sono considerati responsabili esterni del trattamento ai sensi dell'art. 28 del GDPR (es.: commercialista, consulente del lavoro, consulente, fornitori di servizi digitali, conservatori di documenti informatici, ecc.).

Informativa

L'avvocato può fornire in un unico contesto, anche **mediante affissione nei locali dello Studio e, se ne dispone, pubblicazione sul proprio sito Internet**, anche utilizzando formule sintetiche e colloquiali, **l'informativa sul trattamento dei dati personali (art. 13 del Regolamento) e le notizie che deve indicare ai sensi della disciplina sulle indagini difensive**.

IL PRINCIPIO DELLA TRASPARENZA

IL LEGISLATORE COMUNITARIO ATTRIBUISCE NUOVI DIRITTI AGLI INTERESSATI E QUINDI IMPONE AI TITOLARI NUOVI OBBLIGHI

con la legge comunitaria vengono posti in capo al TITOLARE (e quindi all'Avvocato) obblighi di TRASPARENZA più stringenti rispetto alla precedente normativa

↓

L'INFORMATIVA

VI E' UN MAGGIOR DETTAGLIO DELLE INFORMAZIONI CHE DEVONO ESSERE RESE ALL'INTERESSATO

Art. 12 GDPR
Linguaggio chiaro preciso
e comprensibile soprattutto se
Il trattamento concerne i minori

Periodo di conservazione o criteri
Utilizzati per determinarli

Diritti dell'interessato:
- accesso, rettifica, cancellazione,
opposizione,limitazione, portabilità
IL CONSENSO PUO' ESSERE REVOCATO

Diritto di proporre reclamo
Autorità di controllo

Esistenza di un processo
Decisionale automatizzato
profilazione

I punti di contatto (ad es. D.P.O.)

Conservazione e Cancellazione dei dati

la **definizione** di un grado di giudizio o la **cessazione** dello svolgimento di un incarico **non** comportano un'automatica dismissione dei dati.

Una volta **estinto il procedimento** o il relativo rapporto di mandato, **atti e documenti** attinenti all'oggetto della difesa o delle investigazioni difensive **possono essere conservati**, in originale o in copia e anche in formato elettronico, qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del Trattamento → (art. 33 co. 3 cod. deontologico)

Se è prevista una **conservazione per adempiere a un obbligo normativo**, anche in materia fiscale e di contrasto della criminalità, sono custoditi i soli dati personali **effettivamente necessari per adempiere al medesimo obbligo**.

Fermo restando quanto previsto dal codice deontologico forense in ordine alla restituzione al cliente dell'originale degli atti da questi ricevuti (art. 33), e salvo quanto diversamente stabilito dalla legge, è consentito, previa comunicazione alla parte assistita, **distruggere, cancellare o consegnare** all'avente diritto o ai suoi eredi o aventi causa la documentazione integrale dei fascicoli degli affari trattati e le relative copie.

In caso di **revoca o di rinuncia** al mandato fiduciario o del patrocinio, **la documentazione** acquisita è **rimessa**, in originale ove detenuta in tale forma, **al difensore che subentra formalmente nella difesa**.

La titolarità del trattamento, fintanto che si conservano i fascicoli, non cessa per il solo fatto della sospensione o cessazione dell'esercizio della professione.

In caso di **cessazione** anche per sopravvenuta incapacità e **qualora manchi un altro difensore** anche succeduto nella difesa o nella cura dell'affare,

la documentazione dei fascicoli degli affari trattati, decorso un congruo termine dalla comunicazione all'assistito, **è consegnata al Consiglio dell'ordine di appartenenza ai fini della conservazione per finalità difensive**.

Con la conclusione del mandato difensivo il trattamento non si conclude automaticamente

L'avvocato potrà decidere di conservare i documenti/dati personali per esigenze difensive sue o del cliente secondo il principio di minimizzazione

Se la conservazione è effettuata per un obbligo di legge (adempimenti fiscali) dovranno essere conservati solo gli atti necessari ad adempiere a tale obbligo

Previa comunicazione al cliente l'avvocato potrà decidere di distruggere, cancellare o consegnare all'avente diritto/eredi tutti gli atti contenuti nel fascicolo

Dopo la cessazione dell'esercizio della professione e in assenza di un nuovo difensore potranno essere consegnati al COA

Trattamenti da parte di investigatori privati

L'investigatore privato organizza il trattamento dei dati personali secondo le modalità di cui all'articolo 2, comma 1.

L'investigatore privato non può intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta dei dati. Tali attività possono essere eseguite esclusivamente sulla base di **apposito incarico conferito per iscritto e solo per le finalità di cui alle presenti regole**

L'atto d'incarico deve menzionare in maniera specifica **il diritto che si intende esercitare** in sede giudiziaria, ovvero **il procedimento penale al quale l'investigazione è collegata**, nonché **i principali elementi di fatto che giustificano l'investigazione** e **il termine ragionevole entro cui questa deve essere conclusa**

L'investigatore privato deve eseguire **personalmente l'incarico ricevuto e può avvalersi solo di altri investigatori privati indicati nominativamente all'atto del conferimento dell'incarico**, oppure successivamente in calce a esso qualora tale possibilità sia stata prevista nell'atto di incarico. Restano ferme le prescrizioni predisposte ai sensi dell’art. 2-septies del d.lgs. n. 196/2003 e art. 21 del d.lgs. n. 101/2018 relative al trattamento delle particolari categorie di dati personali di cui all’art. 9, par. 1, del Regolamento (UE) 2016/679

Nel caso in cui si avvalga di persone autorizzate al trattamento dei dati per suo conto, **l'investigatore privato rende specifiche istruzioni in ordine alle modalità da osservare e vigila, con cadenza almeno settimanale, sulla puntuale osservanza delle norme di legge e delle istruzioni impartite**. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione a essi richiesta.

Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

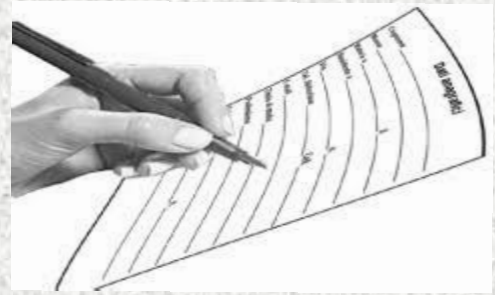
Conservazione e cancellazione dei dati

Nel rispetto dell'art. 5 del Regolamento (UE) 2016/679, i dati personali trattati dall'investigatore privato possono essere **conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto**. A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico, i quali possono consentire, anche in sede di mandato, l'eventuale conservazione temporanea di materiale strettamente personale dei soggetti che hanno curato l'attività svolta, ai soli fini dell'eventuale dimostrazione della liceità, trasparenza e correttezza del proprio operato. Se è stato contestato il trattamento il difensore o il soggetto che ha conferito l'incarico possono anche fornire all'investigatore il materiale necessario per dimostrare la liceità, trasparenza e correttezza del proprio operato, per il tempo a ciò strettamente necessario

La sola pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, **non** costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

DIRITTI DELL'INTERESSATO



L'interessato dovrà essere informato dei suoi diritti e sulle relative modalità di esercizio e precisamente sull'esistenza del diritto di chiedere al titolare

- l'accesso ai dati personali
- La rettifica e la cancellazione degli stessi
- La limitazione del trattamento
- Il diritto di opporsi al trattamento
- Il diritto di portabilità dei dati
- Possibilità di proporre reclamo all'Autorità di controllo

IL DIRITTO ALL'OBLIO --- ART. 17

Il **diritto all'oblio** viene inserito per la prima volta in una norma e diviene un principio fondamentale (in passato era già stato introdotto da alcune pronunce della Corte di Giustizia e della Corte di Cassazione)

l'interessato potrà chiedere al titolare di cancellare i propri dati personali anche on-line qualora ricorrano le seguenti condizioni

1) se i dati sono trattati solo sulla base del consenso
2) se i dati non sono più necessari per le iniziali finalità
3) se i dati sono trattati illecitamente
4) se vi è opposizione al trattamento

Diritto all'oblio: la riabilitazione del reo, condannato per un reato 10 anni prima, fa sorgere il suo diritto a richiedere la rimozione degli url relativi alle notizie sulla sua condanna

Provvedimento del 24.7.19 n. 153

Per l'Avvocato il diritto all'oblio non potrà essere esercitato sino quando non sia maturato il termine di prescrizione dell'azione per la responsabilità professionale. È importante rilevare, inoltre, che l'esercizio del diritto in parola cede il passo di fronte all'adempimento di alcuni obblighi di archiviazione dei dati per periodi specifici e risulta pertanto non utilmente esercitabile ove comprometta l'adempimento ad obblighi fiscali o si ponga in contrasto necessità archivistiche di pubblico interesse ovvero, infine, ove il mantenimento del dato sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria

DIRITTO ALLA PORTABILITA’ DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).
Costituisce a ben vedere uno sviluppo del diritto d’accesso.
In prima approssimazione si può affermare che l’esercizio del diritto alla portabilità consente all’interessato di ottenere dal titolare del trattamento i dati personali in un formato strutturato d’uso comune e leggibile ovvero il trasferimento di detti dati dall’originario titolare del trattamento ad un altro.
La portabilità facendo circolare dati personali direttamente tra i titolari del trattamento agevola lo sviluppo di un mercato concorrenziale dei servizi della società dell’informazione.
Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al titolare *(si veda il considerando 68 per maggiori dettagli)*.
Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Linee-guida sul diritto alla "portabilità dei dati" - WP242
adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016
Adottate il 13 dicembre 2016
Versione emendata e adottata il 5 aprile 2017

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 5 aprile 2017

Il diritto alla portabilità dei dati

La scheda presenta il diritto alla portabilità dai dati in relazione a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee-guida del WP29

COSA È?

È un diritto innovativo previsto dall'articolo 20 del regolamento (Ue) 2016/679 che consente all'interessato **di ricevere i dati personali forniti a un titolare**, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di **trasmetterli a un altro titolare** del trattamento senza impedimenti.

QUALI VANTAGGI PUO' OFFRIRE?

- **facilitare il passaggio** da un fornitore di servizi all'altro;
- consentire la **creazione di nuovi servizi** nel quadro della strategia dell'Ue per il mercato unico digitale;
- offrire la possibilità di **«riequilibrare» il rapporto fra interessati e titolari del trattamento** tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

COSA PERMETTE DI FARE?

- **ricevere dati personali** trattati da un titolare e conservarli su un supporto personale o un *cloud* privato in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli necessariamente a un altro titolare *(es: recuperare l'elenco dei brani musicali preferiti detenuto da un servizio di musica in streaming, per scoprire quante volte si sono ascoltati determinati brani);*
- **trasmettere dati personali** da un titolare del trattamento a un altro titolare del trattamento *(es.: un diverso fornitore di servizi).*

L'esercizio del diritto alla portabilità dei dati **non pregiudica nessuno degli altri diritti** dell'interessato, che può, per esempio:

- **continuare a fruire del servizio** offerto dal titolare anche dopo un'operazione di portabilità;
- **esercitare il diritto di cancellazione** *(o «diritto all'oblio»)* ai sensi dell'art. 17 del regolamento.

QUANDO TROVA APPLICAZIONE?

Per essere portabili i dati devono:

- essere **dati personali chiaramente riferibili all'interessato.** Sono quindi ad esempio esclusi i dati anonimi;
- essere **trattati sulla base del consenso preventivo** dell'interessato o di un **contratto** di cui è parte l'interessato;
- essere **trattati attraverso strumenti automatizzati.** Sono quindi esclusi gli archivi e registri cartacei;
- essere stati **forniti consapevolmente** e in modo attivo dall'interessato *(ad es., i dati di registrazione inseriti compilando un modulo online, come indirizzo postale, nome utente, età, ecc.).*
- Sono compresi anche i **dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo** *(es.: la cronologia delle ricerche effettuate dall'interessato, i dati relativi al traffico, i dati relativi all'ubicazione, dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness.)*

Il diritto alla portabilità **non si applica** invece ai «dati inferenziali» né ai «dati derivati» *(es.: l'esito di una valutazione concernente la salute di un utente o il profilo creato al fine di attribuire uno score creditizio o di ottemperare a normativa antiriciclaggio).*

L'esercizio del diritto alla portabilità **non deve ledere i diritti e le libertà altrui.**

I dati portabili **devono essere forniti in un formato «interoperabile»**, ossia in un formato che ne consenta il riutilizzo. I titolari potranno utilizzare formati di impiego comune, se già esistenti, oppure utilizzare formati aperti (es. XML), ovvero sviluppare formati interoperabili e strumenti informatici che consentano di estrarre i dati pertinenti.

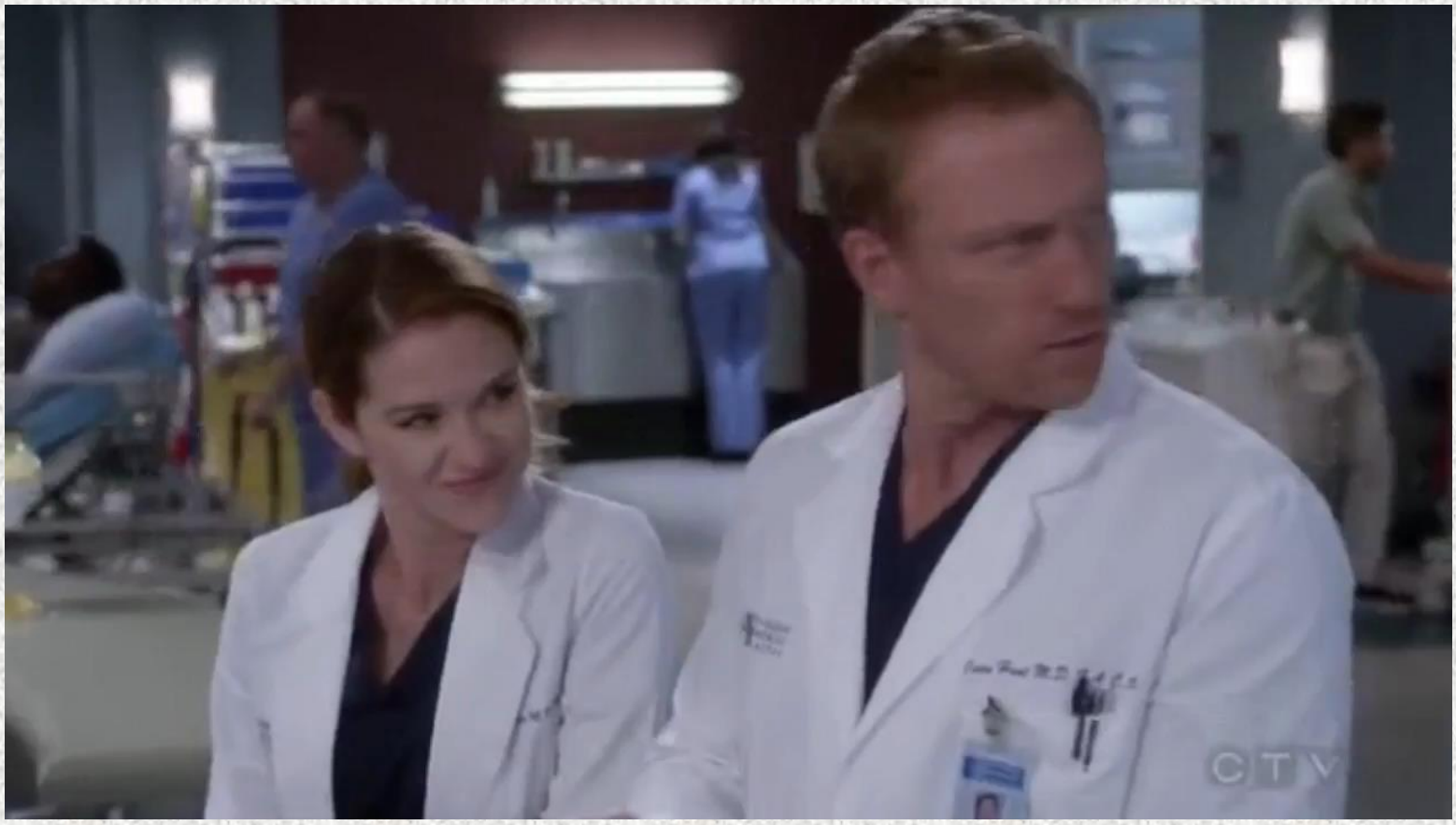
La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento.
Per un quadro completo si invita a consultare la pagina www.garanteprivacy.it/regolamentoue/portabilita

Ciò significa che l'Avvocato che tratti i dati dei clienti *con mezzi automatizzati* (per esempio, adottando un gestionale informatico o anche solo tenendo uno schedario sotto forma di foglio di calcolo) è tenuto a comunicare i dati del suo cliente al collega alle seguenti condizioni:
- il cliente abbia fornito il consenso al trattamento dei suoi dati personali o il trattamento sia necessario per l'esecuzione di un contratto di cui il cliente è parte;
- il trattamento sia stato effettuato con mezzi automatizzati.

Pertanto, se il cliente richiede la trasmissione dei suoi dati ad un collega, l'Avvocato dovrà trasferirli in **formato strutturato comunemente usato e leggibile da una macchina**.

L'Avvocato dovrà pertanto essere in grado di seguire e identificare i destinatari dei dati personali che elabora compulsando l'apposito registro dei trattamenti.

VIOLAZIONE INFORMATICA (DATA BREACH)



VIOLAZIONE INFORMATICA (DATA BREACH)

L'art. 33 del Regolamento Europeo 679/2016 introduce una grossa novità nello scenario della sicurezza dei dati: in particolare il titolare del trattamento nel caso di violazione **dei propri sistemi informatici (c.d. data breach) dovrà notificare detta violazione senza giustificato ritardo e comunque ove possibile entro 72 ore** da cui si viene a conoscenza della violazione

- CASI REALI DI DATA BREACH CONSISTENTI

- JP Morgan, banca internazionale, con la sottrazione di quasi 79 milioni di record
- E-bay, piattaforma di e-commerce, che si è vista sottrarre 145 milioni di record
- Gruppo Benetton, multinazionale di abbigliamento che ha visto trafugati le bozze di una collezione
- Sony, trafugati più di 30 milioni di record con il fermo dei sistemi per 3 giorni

Questi sono solo alcuni dei casi, i più noti perché portati all'onore delle cronache, che **hanno visto le aziende essere protagoniste di attacchi informatici**. In realtà miglia e migliaia sono le imprese, anche piccole o piccolissime, che sono state oggetto di attacchi informatici che hanno compromesso la sicurezza dei loro sistemi.

QUALI SONO GLI ADEMPIMENTI DOPO AVER SUBITO UN DATA BREACH?

1 – Descrivere la natura della violazione dei dati personali compresi, *ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*

Questo punto presuppone la presenza in azienda di **personale informatico adeguatamente preparato** oppure un servizio esterno con qualche bravo sistemista (meglio se con un contratto che citi espressamente questo punto).

Inoltre **è necessaria la presenza di policy aziendali** che permettano all'azienda di avere sempre contezza del numero degli interessati di cui si tratta i dati e delle relative registrazioni di dati.

2 – Comunicare il nome e i dati di contatto del responsabile della protezione dei dati *o di altro punto di contatto presso cui ottenere più informazioni;*

Il Data Protection Officer o altro incaricato preventivamente nominato diventa il punto di contatto con il Garante.

3 – Descrivere le probabili conseguenze della violazione dei dati personali;

Indipendentemente da un obbligo di legge, sarebbe opportuno **verificare preventivamente quali siano i rischi nel trattare i dati**. Avere chiari i pericoli ed i rischi è importante anche nel trattare i dati.

4 – Descrivere le misure adottate *o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi*

Anche in questo caso, **andare ad identificare che misure adottare in piena crisi**, a seguito di un evento dannoso, in un momento in cui si è nel mirino del Garante ed avendo poco tempo (72 ore –3 giorni- dalla scoperta dell'evento) **risulta molto difficile ed impegnativo**. Molto meglio analizzare la questione preventivamente ed **individuare una serie di miglioramenti alle proprie misure di sicurezza** che potrebbero essere implementati nel tempo e che **possono evitare data breach.**

Registro delle attività di trattamento

L’art. 30 del GDPR prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.

E’ un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all’interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Sono obbligati alla tenuta del Registro:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare **un rischio – anche non elevato – per i diritti e le libertà dell'interessato**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti non occasionali**;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD**.

Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.

In quanto tale, il registro deve essere **mantenuto costantemente aggiornato** poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere **compilato sia in formato cartaceo che elettronico** ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento.

Registro delle attività di trattamento
(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

TITOLARE DEL TRATTAMENTO	Studio Legale XY	**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	Dott. Mario Rossi
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

	TRATTAMENTO					DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Responsabile	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

LA NUOVA FIGURA DEL DPO

Il nuovo Regolamento Europeo riconosce nel D.P.O. uno degli elementi chiave all'interno del nuovo sistema di governance dei dati fondato sul principio dell'accountability e prevede una serie di condizioni in rapporto alla nomina, allo stato e hai compiti specifici di questa nuova figura.
I responsabili della protezione dei dati (D.P.O.) sono al centro di questo nuovo quadro giuridico in molti ambiti e sono **chiamati a facilitare l'osservanza delle disposizioni del regolamento:**

- oltre a favorirne l'osservanza attraverso strumenti di accountability (supportando la valutazione di impatto e conducendo o supportando audit in materia di protezione dei dati)

- i DPO fungono da interfaccia tra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno dell'azienda o di un ente.

Al titolare o al responsabile del trattamento spetta il compito fondamentale di **consentire lo svolgimento efficace dei compiti cui il DPO** è preposto: la nomina di un DPO è solo il primo passo perché lo stesso dovrà disporre anche di **autonomia risorse** sufficienti a svolgere in modo efficace i compiti cui è chiamato.

LE LINEE GUIDA DEL GARANTE

LE LINEE GUIDA SUL DPO

Il **13 dicembre 2016** il Gruppo dei Garanti europei ha emanato le prime linee guida sul responsabile della protezione dei dati che specificano i requisiti soggettivi e oggettivi di questa figura.

Nel documento vengono specificate le condizioni in cui scatta **l'obbligo di nomina** del DPO (anche attraverso esempi concreti) le **competenze professionali** e le **garanzie di indipendenza e inamovibilità** di cui il DPO deve godere nello svolgimento delle proprie attività di indirizzo e controllo all'interno dell'organizzazione del titolare.

NOMINA OBBLIGATORIA DEL DPO

CASI IN CUI E' OBBLIGATORIA LA NOMINA DEL DPO
In base all'articolo 37 primo paragrafo del Regolamento Europeo la nomina del DPO è obbligatoria in **tre casi** particolari:

1) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;

2) se le **attività principali** del titolare o del responsabile consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico di interessati su larga scala**;

3) se le attività principale del titolare o del responsabile consistono nel **trattamento su larga scala** di dati personali che rivelano l'origine razziale o etnica le opinioni politiche le convinzioni religiose o filosofiche l'appartenenza sindacale nonché di dati genetici dati biometrici dati relativi alla salute e alla vita sessuale o all'orientamento sessuale della persona o di dati personali relativi a condanne penali e reati (art. 9 “categorie particolari di dati).

COSA FARE SE SI DECIDE DI NON NOMINARE IL DPO

Tranne quando sia evidente che un soggetto non è tenuto a nominare il dpo i titolari e responsabili devono **documentare le valutazioni compiute all'interno dell'azienda** per stabilire se si applichi o meno l'obbligo di nomina di un DPO così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione (e in base a l'obbligo di dotarsi delle politiche del trattamento dei dati ai sensi dell'articolo 24 GDPR).

Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario per esempio se il titolare o il responsabile intraprendono nuove attività o forniscono nuovi servizi ad alto contenuto tecnologico che potrebbero ricadere nel novero dei casi elencati all'articolo 37 paragrafo 1 GDPR sulla nomina obbligatoria del DPO

QUALI SONO I PRESUPPOSTI DI OBBLIGATORIETA'

Art. 37 comma 1 lettera B): il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogni qualvolta **le attività principali del titolare del trattamento e del responsabile del trattamento** consistano in trattamenti che per loro natura ambito di applicazione e/o finalità richiedano il **monitoraggio regolare e sistematico degli interessati su larga scala**.

Nel considerando 97 si afferma che le attività principali di un titolare del trattamento: "riguardano le sue **attività primarie** ed esulano dal trattamento dei dati personali le attività accessorie".
Con attività principali si possono intendere le **operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento**.

D'altro canto tutti gli organismi pubblici e privati svolgono determinate attività quali ad esempio il pagamento delle retribuzioni al personale che pur essendo necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo devono essere considerate solitamente accessorie e non vengono annoverate fra le attività principali

MONITORAGGIO SU LARGA SCALA

Sulla base delle linee guida possiamo ritenere che si possa parlare di trattamento su larga scala nei seguenti casi:

a) numero di soggetti interessati cui i dati si riferiscono (in termini o di preciso numero o di percentuale rispetto a una rilevante porzione della popolazione)

b) ammontare/grandezza dei database e del volume delle informazioni trattate;

c) durata o indefinitività delle attività di trattamento dei dati

d) estensione geografica delle attività di trattamento

PRESUPPOSTI DI OBBLIGATORIETA'

Alcuni esempi di soggetti che svolgono trattamenti su larga scala:

1) trattamento di dati di pazienti da parte di un ospedale

2) trattamento di dati di viaggiatori che utilizzano un sistema di trasporto pubblico

3) trattamento in tempo reale di dati di geolocalizzazione di clienti di una catena di fast food per fini statistici

4) trattamento di dati della clientela da parte di una banca ad una compagnia di assicurazioni nel normale svolgimento delle relazioni contrattuali e commerciali con dei clienti

5) trattamento di dati di utenti di un motore di ricerca ai fini di analisi comportamentale a scopi di marketing

6) trattamento di dati di traffico di ubicazione e dei contenuti della clientela da parte degli internet Service providers

COSA SI INTENDE PER MONITORAGGIO "REGOLARE O SISTEMATICO"

Per **monitoraggio regolare** i garanti dell'Unione Europea forniscono tale interpretazione

1) Continuo o ad intervalli determinati per particolari periodi di tempo
2) ricorrente a scadenze di tempo fisso
3) Comunque costante e avente luogo periodicamente

Per **monitoraggio sistematico** essi forniscono tale interpretazione

1) basato su un sistema metodico organizzato e preconfigurato
2) avente luogo come parte di un piano generale di raccolta dei dati personali
3) effettuato come parte di una qualsiasi strategia

ESEMPI DI MONITORAGGIO REGOLARE E SISTEMATICO

- Gestione operativa di una rete di telecomunicazioni
- fornitore di servizi di telecomunicazione
- profilazione e scoring ai fini di Risk Assessment (ad esempio per scopi di credit scoring, fissazione di premi assicurativi, prevenzione di frodi, prevenzione di antiriciclaggio)
- Tracciatura della posizione geografica attraverso app sul cellulare
- programmi di fidelizzazione
- pubblicità comportamentale
- monitoraggio del benessere della Salute
- monitoraggio dello stato della forma fisica e dello stato sanitario attraverso dispositivi indossabili o portatili
- televisioni a circuito chiuso
- sistemi di home authentication
- veicoli Smart

OBBLIGO DI NOMINA DEL DPO RAPPORTI TRA TITOLARE E RESPONSABILE DEL TRATTAMENTO

Per quanto riguarda la nomina del DPO l'articolo 37 **non distingue tra titolare o responsabile del trattamento**. Potrà essere il solo titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro, a dover nominare un DPO.
Questi ultimi saranno poi tenuti alla reciproca collaborazione

Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oppure all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati su larga scala in considerazione del ridotto numero di clienti della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare svolge nel suo complesso trattamenti su larga scala.
Ne deriva che il responsabile deve nominare un DPO ai sensi dell'articolo 37 primo paragrafo lettera B al contempo l'azienda in quanto tale non è soggetta all'obbligo di nomina del DPO

CARATTERISTICHE DEL DPO

Il Data Protection officer **non deve ricevere** dal titolare o dal responsabile del trattamento **delle istruzioni** per quanto riguarda l'esecuzione dei compiti affidatigli (e figura del tutto autonoma) **ne è soggetto** al **potere disciplinare** sanzionatorio per l'adempimento dei propri compiti (ad esempio in ciò, tra l'altro, risiedono i caratteri distintivi tra data Protection officer e responsabile del trattamento che al contrario deve ricevere istruzioni scritte del soggetto al controllo e all'autorità del titolare del trattamento Ivi compresi i profili sanzionatori).

Va **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali, deve avere le **risorse necessarie ed il potere di spesa** per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica (ad esempio **spese per il suo aggiornamento professionale**).

L'articolo 39 del regolamento individua il nucleo minimo (che comunque può essere anche esteso) dei compiti assegnati al responsabile della protezione dei dati

COMPITI E FUNZIONI DEL DPO

Il DPO è incaricato almeno dei seguenti compiti

1) informare e **fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi di legge sulla protezione dei dati

2) **sorvegliare l'osservanza del regolamento** e delle altre leggi (sia UE che nazionali) sulla protezione dei dati nonché delle politiche del titolare del trattamento e del responsabile del trattamento in materia di protezione dei dati personali compresi l'attribuzione delle responsabilità la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo

3) fornire se richiesto un **parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliare lo svolgimento

4) **cooperare con il garante fungendo altresì da punto di contatto** sulle questioni connesse al trattamento tra cui la consultazione preventiva ed effettuare se del caso consultazioni relativamente a qualunque altra questione

IL DPO RIFERISCE DIRETTAMENTE AL VERTICE ANZIENDALE

Il DPO deve avere un **rapporto continuo e diretto con i vertici aziendali**
Per vertice gerarchico si intende il vertice amministrativo-gestionale cioè ad esempio il consiglio di amministrazione.

Il DPO non solo deve riferire cioè mettere a conoscenza il consiglio di amministrazione delle indicazioni e delle raccomandazioni da lui fornite nel quadro delle sue funzioni di informazione consulenza a favore del titolare o del responsabile del trattamento ma deve altresì redigere una **relazione annuale** delle attività svolte da sottoporre al CDA

Non solo, il rapporto e le interlocuzioni tra il DPO e il vertice gerarchico possono esplicarsi anche come segue: se il titolare o il responsabile assumono decisioni incompatibili con il Regolamento Europeo e che disattendono le indicazioni/consulenze/richieste fornite dal DPO quest'ultimo deve avere la possibilità di **manifestare il proprio dissenso** al più alto livello del management ad esempio facendo verbalizzare in CDA il suo dissenso e facendo pervenire una relazione al più alto livello del management

COME VA COINVOLTO IL DPO

L'azienda deve assicurare il tempestivo e immediato coinvolgimento del DPO tramite la sua informazione/consultazione fin dalle fasi iniziali di qualsiasi progetto;
il DPO deve essere annoverato tra gli interlocutori da consultare all'interno dell'azienda da parte di tutti i reparti aziendali;
il DPO deve partecipare ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento. Ciò significa che occorrerà garantire per esempio:
- che il DPO sia invitato a partecipare su base regolare alle riunioni del Management di alto e medio livello;
- la presenza del DPO ogniqualvolta devono essere assunte decisioni che impattano sulla protezione dei dati.
- Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del DPO riceva sempre la dovuta considerazione.
In caso di disaccordi vanno documentate le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO
- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente

RGPD

REGOLAMENTO (UE) 2016/679

Valutazione d'impatto sulla protezione dei dati (DPIA)

Classificazione dei RISCHI

classi di rischi (in relazione all'effetto della minaccia sulle caratteristiche dell'informazione)		classificazioni di altre fonti	
		linee guida wp 29	art 32 GDPR
1	Riservatezza	accesso illegittimo	divulgazione/accesso non autorizzato
2	Integrità	modifica indesiderata	modifica
3	Disponibilità	scomparsa dei dati	distruzione perdita

classi di rischi (in relazione alla fonte della minaccia)	
U	comportamento umano
S	eventi relativi agli strumenti
C	eventi relativi al contesto

Elenco Rischi-minacce

classe rischio		rischio di dettaglio (possono essere ripetuti per più categorie)
RD	U	replica dei dati su supporto non sicuro/adatto
R	U	installazione di software non autorizzato sulla postazione di lavoro
R	U	divulgazione involontaria delle informazioni (es in un dialogo)
R	U	attacco di ingegneria sociale per carpire informazioni/furto identità
R	U	mancata protezione dei pc (es. schermi non protetti)
R	U	cambio mansione, dimissioni di dipendente
R	U	affidamento di attività di progetto/servizio a fornitori
RID	S	infezioni da virus/malware
R	S	sistema di autenticazione/profilazione/gestione delle credenziali non adeguato
RID	S	errori/vulnerabilità nel software utilizzato
R	S	trasmissioni di dati in maniera non sicura
I	S	installazione di un middleware, software o hw che danneggia i dati
RI	U	comportamenti sleali o fraudolenti di dipendenti
ID	US	errori in fase di aggiornamento dei SO, del middleware, delle configurazioni
ID	U	errori umani involontari di dipendenti (es per poca formazione/competenza, disattenzione, ..)
D	C	evento naturale catastrofico (incendio, inondazione)
D	C	evento vandalico
RD	C	furto di dispositivi (pc, telefono, hw)
D	U	utilizzo di sw contraffatto
D	U	dimensionamento non corretto dei repository dei dati (DB, file system)
D	U	errori in fase di aggiornamento dei sw applicativo
D	U	scadenza licenza, mancato aggiornamento middleware
D	C	interruzioni o non disponibilità della rete (guasti)
D	U	indisponibilità del personale (malattia, sciopero, pensionamento, ..)
D	C	furto documenti cartacei
D	S	guasto hardware
D	S	attacchi DOS/DDOS
D	C	interruzioni o non disponibilità dei sistemi complementari (elettricità, climatizzazione, ecc.)

Il foglio riporta un elenco non esaustivo delle misure che possono essere adottate per ridurre i rischi. E' necessario valutare di volta in volta quali misure sono utilizzabili a riduzione dei singoli rischi. Le misure sono tratte da CNIL - tool di valutazione d'impatto sulla privacy

tipologia di misura	misura	descrizione/esempi
controlli di sicurezza funzionali	crittografia	mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.)
controlli di sicurezza funzionali	anonimizzazione	
controlli di sicurezza funzionali	partizionamento dei dati	
controlli di sicurezza funzionali	controllo degli accessi	
controlli di sicurezza funzionali	tracciabilità	es gestione dei log
controlli di sicurezza funzionali	archiviazione	processi di gestione dell'archivio (consegna, archiviazione, consultazione etc.). Specificare i ruoli relativi all'archivio (ufficio di origine, agenzie di trasferimento etc.) e la politica di archiviazione.
controlli di sicurezza funzionali	sicurezza dei documenti cartacei	sono definite le regole per la conservazione dei documenti cartacei contenenti dati utilizzati durante il trattamento, come sono stampati, archiviati, distrutti e scambiati.
controlli di sicurezza funzionali	minimizzazione della quantità dei dati personali	rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati

controlli di sicurezza fisici	minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento	(es politiche di aggiornamento del software, test del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali)
controlli di sicurezza fisici	controlli per infezioni da malware e virus	(misure per proteggere l'accesso di infezioni a reti, postazioni, server)
controlli di sicurezza fisici	gestione delle postazioni di lavoro	Misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accesso, lavoro su uno spazio di rete di backup, controlli di integrità logging etc.).
controlli di sicurezza fisici	backup	Politiche e mezzi implementati per assicurare la disponibilità o l'integrità dei dati personali, mentre si mantiene la loro confidenzialità
controlli di sicurezza fisici	manutenzione delle infrastrutture	politica di manutenzione fisica degli apparati IT e dei sistemi complementari
controlli di sicurezza fisici	contratti di trattamento	Regolare i rapporti di approvvigionamento (es. responsabile trattamento dati, responsabile protezione dei dati, servizi cloud, ecc) tramite un contratto che riporti ad esempio: - Richiedere al fornitore di inoltrare la sua politica di sicurezza dei sistemi informativi insieme a tutti i documenti di supporto delle sue certificazioni di sicurezza delle informazioni e allegare tali documenti al contratto. Garantire che le misure siano conformi alla propria politica di sicurezza ed alle raccomandazioni dell'autorità garante. - Determinare e fissare in modo preciso, su base contrattuale, le operazioni che il responsabile del trattamento potrà eseguire sui dati personali: 1) I dati a cui avrà accesso o che gli saranno trasmessi. 2) Le operazioni che deve eseguire sui dati. 3) La durata per la quale può memorizzare i dati. 4) Tutti i destinatari a cui il responsabile del trattamento potrà trasmettere i dati. 5) Le operazioni da eseguire al termine del servizio (cancellazione permanente dei dati o restituzione dei dati nel contesto della reversibilità quindi distruzione di dati). 6) Gli obiettivi di sicurezza stabiliti dal titolare del trattamento. - Determinare, su base contrattuale, la ripartizione delle responsabilità in merito ai processi legali volti a consentire agli interessati di esercitare i propri diritti. Esplicitamente vietare o regolare l'utilizzo di fornitori di secondo livello. - Chiarire nel contratto che il rispetto degli obblighi di protezione dei dati è un requisito vincolante del contratto.

controlli di sicurezza fisici	monitoraggio delle attività di rete (incidenti di sicurezza)	Esistenza di misure messe in atto per essere in grado di rilevare tempestivamente incidenti relativi a dati personali e di disporre elementi utilizzabili per studiarli o fornire elementi di prova nel contesto delle indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati etc.)
controlli di sicurezza fisici	controlli degli accessi fisici	Politiche per assicurare la sicurezza fisica (zonizzazione, accompagnamento, uso di tornelli, porte chiuse e così via). Procedure di avviso in caso di irruzione.
controlli di sicurezza fisici	sicurezza dell'hardware	Esistenza delle misure adottate per ridurre la possibilità che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili etc.) vengano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso etc.)
controlli di sicurezza fisici	Evitare le fonti di rischio	Esistenza di misure per prevenire le fonti di rischio, umane o non umane, che possono essere incontrate a scapito dei dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE etc.)
controlli di sicurezza fisici	Protezione contro fonti di rischio non umane	Esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendio, danni provocati dall'acqua, incidenti interni o esterni, animali, etc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, rilevamento, protezione etc.

controlli d'organizzazione	Organizzazione privacy	Esistenza di un'organizzazione in grado di dirigere e controllare la protezione dei dati personali all'interno dell'organizzazione (designazione di un DPO, creazione di un organo di monitoraggio, etc.)
controlli d'organizzazione	Politiche privacy	Il titolare del trattamento dei dati deve disporre di una banca dati documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (rischi, principi chiave da seguire, obiettivi, regole da applicare, ecc., revisione periodica della politica IT etc.)
controlli d'organizzazione	Gestione dei rischi sulla privacy	Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate (censimento del trattamento dei dati personali, quali dati sono, valutazione del rischio, determinare misure esistenti o previste etc.)
controlli d'organizzazione	Integrare la protezione della privacy nei progetti	Esistenza di procedure che descrivono i metodi per tenere conto della protezione dei dati personali in qualsiasi nuovo trattamento (etichette di fiducia, norme, gestione del rischio per la persona interessata secondo una metodologia etc.)
controlli d'organizzazione	Gestire le violazioni dei dati personali	Esistenza di un'organizzazione oeprativa per rilevare e gestire eventi che possono influire sulle libertà e sulla privacy delle persone interessate (definizione delle responsabilità a piano di reazione, caratterizzazione delle violazioni etc.)
controlli d'organizzazione	Gestione del personale	Esistenza di un piano di formazione in materia di potezione dei dati e procedure/istruzioni che descrivono le istruzioni per l'accesso ai dati .
controlli d'organizzazione	Relazioni con terze parti	Esistenza di una procedura per ridurre i rischi che l'accesso legittimo ai dati da parte di terzi possa porre alle libertà della vita privata delle persone interessate (identificazione dei terzi, contratto di subappalto, convenzione etc.)
controlli d'organizzazione	supervisione	Esistenza di misure per fornire una visione globale e aggiornata dello stato di protezione dei dati e conformità con il GDPR (per monitorare la conformità di trattamenti, obiettivi e indicatori, responsabilità ,etc).

TABELLE DI SUPPORTO PER LA VALUTAZIONE

Valutazione dell'Impatto

Impatto	Livello	descrizione
5	Grave	Individui che possono avere conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).
4	Significativo	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdita significativa di denaro, inserimento di liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
3	Moderato	Gli interessati possono incontrare significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
2	Minore	Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (perdita di tempo per reinserire informazioni, fastidio, irritazioni, ecc.).
1	Irrilevante	Gli interessati non incontrano inconvenienti significativi

Valutazione della probabilità

Probabilità	Liv.	Criterio probabilistico (prob. di accadimento stimata nell'anno)
5	Quasi certo	Prob.>50%
4	Probabile	20%<Prob.<50%
3	Moderata	5%<Prob.<20%
2	Improbabile	1%<Prob.<5%
1	Rara	Prob.<1%

Valutazione dell'efficacia del presidio

l'efficacia del presidio misura quanto è rilevante nella riduzione del rischio tutto ciò che è stato predisposto come misure di sicurezza tecniche o organizzative (cfr foglio misure)

Liv. (score)	Descrizione
5	Il presidio/l'azione costituisce efficace strumento di neutralizzazione
4	Il presidio/l'azione è piuttosto efficace
3	Presidio/azione efficace di circa il 50%
2	Presidio/azione efficace in minima parte
1	Presidio/azione inefficace: rischio quasi invariato o invariato

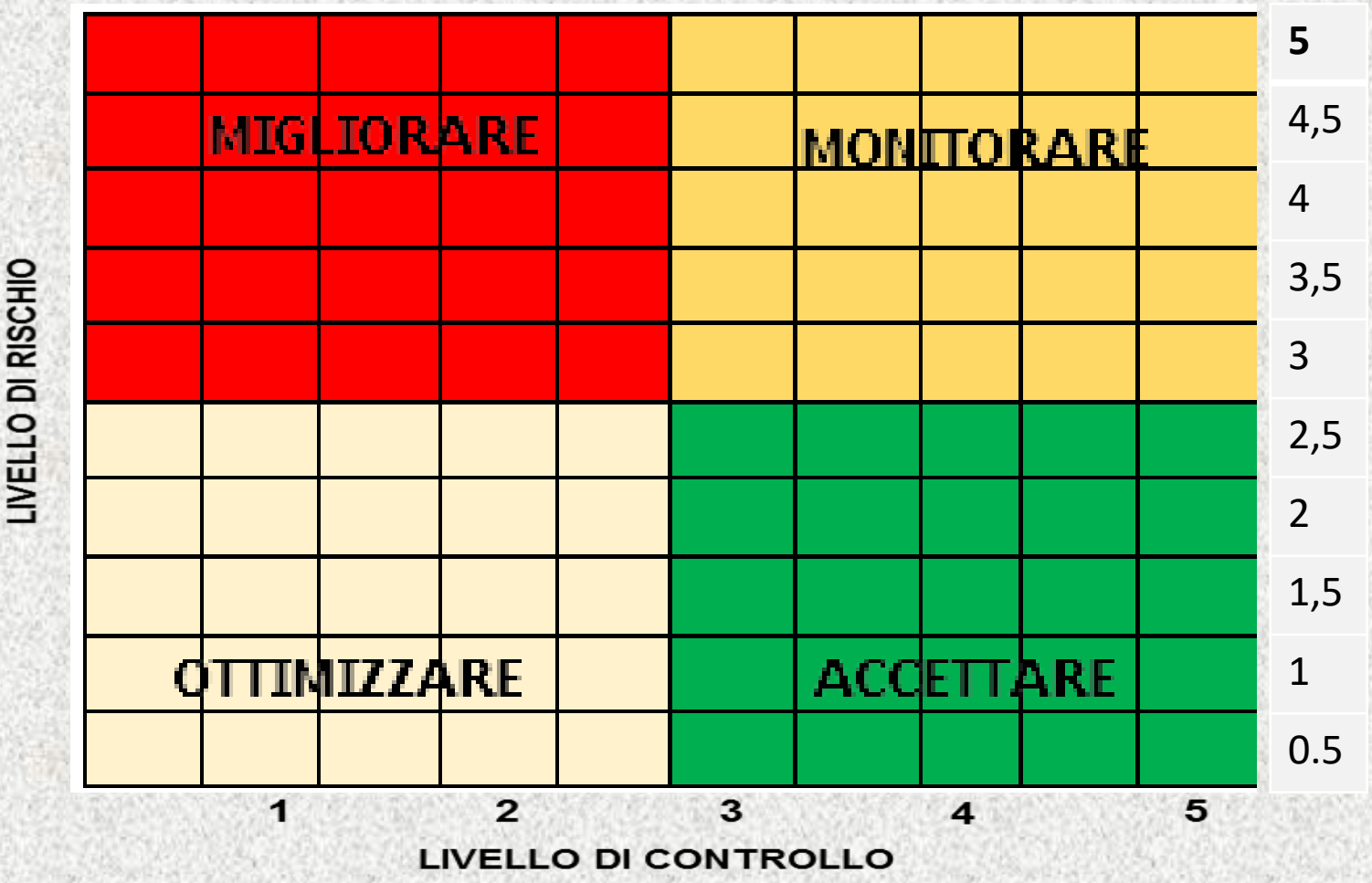
Formule di Calcolo del Rischio

Rischio inerente= $\sqrt{Impatto\ x\ Probabilità}$

Rischio Residuo= $\sqrt{Impatto\ x\ Probabilità\ x\ \left(1 - \frac{efficacia\ presidio}{5{,}3334}\right)}$

Livello di rischio: $\sqrt{Impatto\ x\ Probabilità}$

Livello di controllo: valore del presidio



Minaccia	Probabilità accadimento (da 1 MIN a 5 MAX)	Impatto (da 1 MIN a 5 MAX)	Efficacia Presidio (Inefficace 1, Massimo 5)	Rischio inerente (impatto*probabilità)	rischio residuo attuale	Risk Rating (*rif. foglio Algoritmi e scale)	Azioni ipotizzate (se rischio attuale sopra soglia)	rischio residuo post trattamento	
furto di apparecchiature (smartphone, pc, server)	2	4	2	2,8	2,2	Migliorare		2,8	

Legenda Risultanze Valutazione

Migliorare. Rischi ad alto livello di esposizione (Rischio Inerente) con un basso livello di presidio. Rappresentano la priorità delle azioni di *risk management* per il miglioramento dei presidi o, alternativamente, i rischi che per scelte di *business* o per loro natura non sono mitigabili e che il *top management* decide consapevolmente di accettare.

Monitorare. Rischi ad alto livello di esposizione (Rischio Inerente) e alto livello di presidio che necessitano di un costante monitoraggio nel tempo al fine di verificare l'evoluzione del rischio inerente e l'efficacia e adeguatezza dei presidi ai fini della loro mitigazione.

Accettare/ Perfezionare. Rischi a basso livello di esposizione (Rischio Inerente) e basso livello di presidio che sono accettati e richiedono una periodica attività di monitoraggio al fine di verificare che il livello di rischio non superi la soglia di tolleranza, per effetto di un innalzamento dell'esposizione potenziale o l'inefficacia/ inadeguatezza dei presidi, che renderebbero necessario un intervento per il loro rafforzamento/ perfezionamento.

Ottimizzare. Rischi a basso livello di esposizione (Rischio Inerente) ed alto livello di presidio. Rappresentano il livello più basso di priorità per azioni di *risk management* con spazi di miglioramento/ efficienza connessi a possibili riduzioni dei costi del controllo.

Foglio di calcolo CSI Piemonte

https://www.google.com/search?q=modello+csi+valutazione+impatto+privacy&oq=modello+&aqs=chrome.0.69i59l2j69i57j35i39j0l2.4745j0j8&sourceid=chrome&ie=UTF-8

Grazie per l’attenzione

PACCHIANA PARRAVICINI E ASSOCIATI
STUDIO LEGALE